Bull. Korean. Math. Soc.
Vol. 17, No. 1, 1980

AN ELEMENTARY PROOF OF SERRE'S CONJECTURE

WUHAN LEE, TAIKYUN KWON AND IN-HO CHO*)

1. Introduction

In this paper, we give an elementary proof of the Serre's Conjecture: If k is a field, is every projective $k[X_1, \ldots, X_n]$-module free? In 1955, this question was asked by J-P Serre[4]. In 1957, Serre[5] proved that every finitely generated projective $A=k[X_1, \ldots, X_n]$ module must be stably free, i. e., $P \oplus A^r \cong A^s$ for suitable natural number r and s. (M. R. Gabel [1] has shownthat if P is not finitely generated, then P is actually free, therefore we restrict P to be a finitely generated $k[X_1, \ldots, X_n]$ module). In terms of algebraic K-theory this means that $K_0(k[X_1, \ldots, X_n]) \cong \mathbf{Z}$. [8]. In view of this, Serre's problem becomes the following: does "stably free" imply free over $A=k[X_1, \ldots, X_n]$?

If $n=1$, then $k[X]$ is a principal ideal domain, so projective $k[X]$-modules are free. In 1958, Seshadri [6] proved that if R is a principal ideal domain, then every finitely generated projective $R[X]$-modules are free. In particular, $R=k[X]$ gives an affirmative answer to Serre's problem when $n=1$ or 2.

There was much interest in this problem for $k \geqq 3$; indeed it was one of the main reasons for the development of algebraic K-theory. Remarkably, the problem was solved simultaneously in January 1976, by Quillen [2] in the United States and Suslin [7] in the Soviet Union.

The basic idea of our elementary proof is due to Lam [1], Quillen [2], Rotman [3], Suslin [7] and Swan [8]. All rings are supposed to be commutative with identity and all modules unitary. We have given much effort for this paper to be as selfcontained and readable as possible.

2. Preliminary results

DEFINITION 1. Let A be a ring and M a A-module. Then $m \in M$ is *unimodular* if there is a A-homomorphism $f: M \to A$ such that $f(m)=1$.

REMARKS. It is clear that $m \in M$ is unimodular if and only if m is a base for a free direct summand of M.

*) Supported by the Ministry of Education Research Fund, 1979-80

Let $a=(a_i)\in A^n$ for some $n\geqq 1$. Then a is unimodular if and only if there exists $b=(b_i)\in A^n$ such that $\sum_{i=1}^{n} a_i b_i=1$. In this case we say that (a_i) is a *unimodular column over A*.

DEFINITION 2. Let A be a ring. A is said to be a *Hermite ring* if any unimodular column over A can be completed to an invertible matrix.

Let F be a free module over a ring A with finite basis $\{e_1, \ldots, e_n\}$. If $a\in F$ is unimodular then there is a finitely generated projective A-module P such that

$$P\oplus Aa=F\cong A^n.$$

We can ask whether $P\cong A^{n-1}$ holds.

PROPOSITION 3. *Let P and a be as above. Then $P\cong A^{n-1}$ if and only if there exists an A-module automorphism $h: F\to F$ such that $h(e_1)=a$.*

Proof. Given an automorphism $h: F\to F$ such that $h(e_1)=a$, we have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Ae_1 & \longrightarrow & F & \longrightarrow & F/Ae_1 & \longrightarrow & 0 \\ & & {\scriptstyle h|Ae_1}\downarrow & & {\scriptstyle h}\downarrow & & \vdots\downarrow & & \\ 0 & \longrightarrow & Aa & \longrightarrow & F & \longrightarrow & F/Aa & \longrightarrow & 0 \end{array}$$

where the two left-side hand maps are isomorphisms, and so by the 5-lemma, the left hand-side map is an isomorphism. Hence

$$P\cong F/Aa\cong F/Ae_1\cong A^{n-1}.$$

The converse is clear.

The proposition can be written in matrix terms as follows: Let

$$a=\sum_{i=1}^{n} a_i e_i$$

Then $P\cong A^{n-1}$ if and only if the unimodular column (a_i) can be extended to an invertible $n\times n$ matrix C. For, given $C=(c_{ij})\in GL(r, A)$ such that $a_i=c_{i1}$ for $i=1, \ldots, n$, i. e., $(a_j)=C\varepsilon_1$, where ε_1 denotes the column vector having first coordinate 1 and 0's elsewhere. Now let h be the corresponding automorphism of the matrix C. Then

$$h(e_1)=\textstyle\sum_{i=1}^{n} c_{i1}e_i=\sum_{i=1}^{n} a_i e_i=a.$$

Therefore $P\cong A^{n-1}$ by Proposition 3. The converse is clear.

THEOREM 4. *Let A be a Hermite ring. Then every stably free A-module is free.*

Proof. Let P be a stably free A-module. Then there exist free A-modules G and F such that

$$P\oplus G=F,\quad G\cong A^r,\quad F\cong A^s$$

for some $r, s\geqq 1$. We prove this by induction on r and so it suffices to prove the case $r=1$. But if $r=1$, it follows from Proposition 3 that P is free, since A is a Hermite ring.

LEMMA 5. *Let A be a ring. Consider polynomials in $A[X]$*

$$f(x)=X^s+a_1X^{s-1}+\ldots+a_s$$
$$g(x)=\qquad b_1X^{s-1}+\ldots+b_s$$

Then, for each j, $1\leqq j\leqq s$, the ideal $(f(x),\ g(x))$ in $A[X]$ contains a polynomial of degree $s-1$ and leading coefficients b_j.

Proof. Define

$$I=\{\text{leading coefficients of those } h(x)\in(f, g) \text{ having degree}\leqq s-1\}.$$

Then I is clearly an ideal in A containing b_1. We prove by induction on j where I contains $b_1, \cdots, b_j$, $j\leq s$. Define

$$g'(x)=Xg(X)-b_1f(X)=\textstyle\sum_i^s(b_{i+1}-b_1a_i)X^{s-i}$$

By induction, I contains the first $j-1$ coefficients of $g'(X)$. the last of which is $b_j-b_1a_{j-1}$. It follows that $b_j\in I$.

3. Main results

THEOREM 6. *Let R be a local ring, $A=R[X]$ and let*

$$\alpha=(a_i)\in A^n$$

be a unimodular column. If some a_i is monic, then α is the first column of an invertible matrix over $R[X]$.

Proof. If $n=1$ or 2, the theorem holds for any commutative ring R. For, let

$$\begin{pmatrix}a_1\\ b_1\end{pmatrix},\quad \begin{pmatrix}a_2\\ b_2\end{pmatrix}\in A^2$$

such that $a_1b_1+a_2b_2=1$, then

$$\begin{pmatrix}a_1 & b_2\\ a_2 & -b_1\end{pmatrix}\begin{pmatrix}b_1 & b_2\\ a_2 & -a_1\end{pmatrix}=\begin{pmatrix}b_1 & b_2\\ a_2 & -a_1\end{pmatrix}\begin{pmatrix}a_1 & b_2\\ a_2 & b_1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

Therefore we may assume $n\geqq 3$. We do an induction on s, the degree of the monic polynomial a_i. By the elementary row operations we may assume a_1 is monic of degree $s>0$ and the other polynomials $a_2, \ldots, a_n$ have degrees $<s-1$. Let $\mathfrak{M}$ be the maximal ideal in R. Thus $\mathfrak{M}A$ consists of those polynomials each of whose coefficients lies in $\mathfrak{M}$. The column $\bar{\alpha}\in A^n/\mathfrak{M}A^n$ is unimodular over $(R/\mathfrak{M})[X]$, so that not all a_i, $i\geqq 2$ lies in $\mathfrak{M}A$. Now assume $a_2\notin\mathfrak{M}A$. Thus, $a_2=r_1X^{s-1}+\ldots+r_s$, and some $r_j\notin\mathfrak{M}$. Since R is a local ring, r_j is a unit. By Lemma 3, the ideal (a_1, a_2) in A contains a monic polynomial of degree $\leqq s-1$, so that the elementary row operation of adding a linear combination of a_1 and a_2 to a_3 produces a monic polynomial of degree $\leqq s-1$ by Lemma 5.

One may now apply the inductive hypothesis.

LEMMA 7. *Let R bea domain, $A=R[X]$ and let*

$$\alpha(X)=(a_i(X))\in A^n$$

be a unimodular column, one of whose coordinate is monic. Then $\alpha(X)=M(X)\alpha(0)$ for some $M(X)\in GL(n, A)$.

Proof. Define

$$I=\{s\in R : u\equiv u' \pmod{sA} \Rightarrow \alpha(u)\sim\alpha(u')\},$$

where $\alpha\sim\beta$ means that α and β are conjugate under the left multiplicative action of $GL(n, A)$.

Then I is an ideal in R : Let $b, b'\in I$ and $r, r'\in R$. If $u, u'\in A$ such that $u-u'=(rb+r'b')a$ for some $a\in A$ then $u-rba=u'+r'b'a$. Thus

$$\alpha(u)\sim\alpha(u-rba)=\alpha(u'+r'b'a)\sim\alpha(u).$$

Therefore I is an ideal in R.

Suppose I is the unit ideal, i. e., $I=R$, then for any u, $u'\in A$, we have $\alpha(u)\sim\alpha(u')$. Therefore we have $\alpha(X)\sim\alpha(0)$, i. e., $\alpha(X)=M(X)\alpha(0)$ for some $M(X)\in GL(n, A)$.

We want prove that the ideal I is the unit ideal. Suppose on the contrary I is a proper ideal in R, so that $I\subset J$ for some maximal ideal J. Since R is a domain, R is contained in the localization R_J. As R_J is local ring and $\alpha(X)\in R_J[X]^n$ is unimodular column one of whose coordinate is monic, so that by Theorem 6, we have

$$\alpha(X)=M(X)\varepsilon_1$$

for some

$$M(X)=(m_{ij}(X))\in GL(n, R_J[X]).$$

Adjoin a new indeterminate Y to $R_J[X]$ and define a matrix

$$N(X, Y)=M(X)[M(X+Y)]^{-1}\in GL(n, R_J[X, Y]).$$

(The matrix $M(X+Y)$ is obtained from $M(X)$ by replacing each of its polynomial entries $m_{ij}(X)$ by $m_{ij}(X+Y)$. If $M(X)^{-1}=(h_{ij}(X))$, then it is easy to see that $(h_{ij}(X+Y))$ is the inverse of $M(X+Y)$). Observe that the definition of $N(X, Y)$ gives $N(Y, 0)=1_n$, the $n\times n$ identity matrix. Since $\alpha(X)=M(X)\varepsilon_1$, it follows that $\alpha(X+Y)=M(X+Y\varepsilon_1$. Therefore,

$$(*)\qquad N(X, Y)\alpha(X+Y)=N(X, Y)M(X+Y)\varepsilon_1=M(X)\varepsilon_1=\alpha(X).$$

Each entry of $N(X, Y)$ is a polynomial in $R_J[X, Y]$, hence may be written as $f(X)+g(X, Y)$ where each monomial in $g(X, Y)$ involves a poritive power of Y. Since $N(X, 0)=1_n$, we must have $f(X)=0$ or 1, and we can conclude that the entries $N(X, Y)$ are polynomials in $R_J[X, Y]$ containing no nonzero monomials of the form sX^i with $i>0$ and $s\in R_J$. Let b be the product of all denominators occuring in coefficients of the polynomial entries of $N(x, y)$. By definition of R_J, we have $b\notin J$ and hence $b\notin I$. Further, $N(X, bY)\in GL(n, R[X, Y])$ for we have just seen that replacing Y by bY eliminates all denominators. Equation $(*)$ gives

$$GL(n, R[X, Y])\alpha(X+bY)=GL(n, R[X, Y])\alpha(X).$$

From this equation it is clear that $b\in I$ which is a contradiction.

LEMMA 8 (Noether). *Let $A=k[X_1, \dots, X_n]$, where k is a field, and let $a\in A$, m be a natural number greater than the total degree of a. Define*

$$Y=X_n$$

and, for $1\leqq i\leqq n-i$ define

$$Y_i=X_i-X_n^{m^{n-i}}.$$

Then $a=ca'$, where $c\in k$ and a' is a monic polynomial over the polynomial ring $k[Y_1, \dots, Y_{n-1}]$.

Proof. Since $\{Y_1, \dots, Y_{n-1}\}$ is a polynomial ring, for the defining equations the Y's give an automorphism of A (with inverse given by $X_n\to X_n$ and $X_i\to X_i+X_n^{m^{n-i}}$ for $1\leqq i\leqq n-1$). The polynomial a may be wirtten

$$a=\Sigma_i a_i X_1^{i1}\dots X_j^{ij}\dots X_n^{in},$$

so

$$a=\Sigma_i a_i(Y_1+Y^{m^{n-1}})^{i_1}\dots(Y_j+Y^{m^{n-j}})^{i_j}\dots(Y_{n-1}+Y^{m^1})_{n-1}Y^{i_n})$$
$$=\Sigma_i a_i(Y^{i_n m^0+i_{n-1}m^1+\cdots+i_j m^{n-j}+\cdots+i_1 m^{n-1}}+$$

terms with Y-degree $< i_n m^0 + i_{n-1} m^1 + \ldots + i_j m^{n-j} + \ldots + i_1 m^{n-1})$.

Since the integers $i_n + i_{n-1} m + \ldots + i_1 m^{n-1}$ have different m-adic expansions, the monomials $a_i Y^{i_n + \cdots + i_j m^{n-1}}$ in a will not cancel out each other and if d is the one with highest degree it will emerge as the leading term in a as a polynomial in Y.

MAIN THEOREM (Quillen–Suslin). *If* $A = k[X_1, \ldots, X_n]$, *where* k *is a field, then every finitely generated projective A-module is free.*

proof. We prove by induction on n. If $n=1$, A is a principal ideal domain, therefore the theorem holds. Every finitely generated projective A-module is stably free[5]. Therefore it suffices to prove that A is a Hermite ring by Theorem 4. Let $\alpha = (a_i)$ be a unimodular column over A. We may assume $a_1 \neq 0$. By Lemma 8, $a = c a_1'$ where $c \in k$ and $a_1' \in k[Y_1, \ldots, Y_{n-1}][Y]$ is a monic polynomial (Y_i defined as in Lemma 8). Since c is a unit, there is no loss of generality in assuming $a_1 = a_1'$, i. e, a_1 is monic. Theorem 7 thus applies to give

$$\alpha(X) = M\alpha(0),$$

where $M \in GL(n, A)$ and $\alpha(0)$ is a unimodular column over a ring $B = R[Y_1, \ldots, Y_{n-1}]$. By induction, B is a Hermite ring, so that $\alpha(0) = N\varepsilon_1$ for some $N \in GL(n, B)$. Hence $MN \in GL(n, A)$ and $\alpha = MN\varepsilon_1$.

References

1. T. Y. Lam, *Serre's Conjecture*, Lecture Notes 635, Springer Verlag, 1978.
2. D. Quillen, *Projective Modules over Polynomial Rings*, Invent. Math. **36** (1976), 167–171.
3. J. J. Rotman, *An introduction to Homological Algebra*, Academic Press, New York, 1979.
4. J. P. Serre, *Paisceaux Algebrique Coherents*, Ann. Math. **61** (1955), 191–278.
5. J. P. Serre, *Modules Projectifs et EspacesFibre's a Fibre Vectorielle*, Sem. Dubrell No. **23** (1957/58)
6. C. S. Seshadri, *Triviality of Vector Bundles over the Affine Space* K^2, Proc. Nat. Acad. Sci. U. S. A., **44** (1958) 456–458.
7. A. A. Suslin, *Projective Modules over Polynomial Ring are Free*, Dokl. Akad. Nauk. SSSR (1976), 235–252.
8. R. G. Swan, *Algebraic K-theory*, Lecture Notes in Math. 76, Springer Verlag, 1968.

Seoul National University
Korea University
Korea University